Phishing Email Analysis Report

Sample 1 :

Sample Email:

PayPal Account Suspension Notice

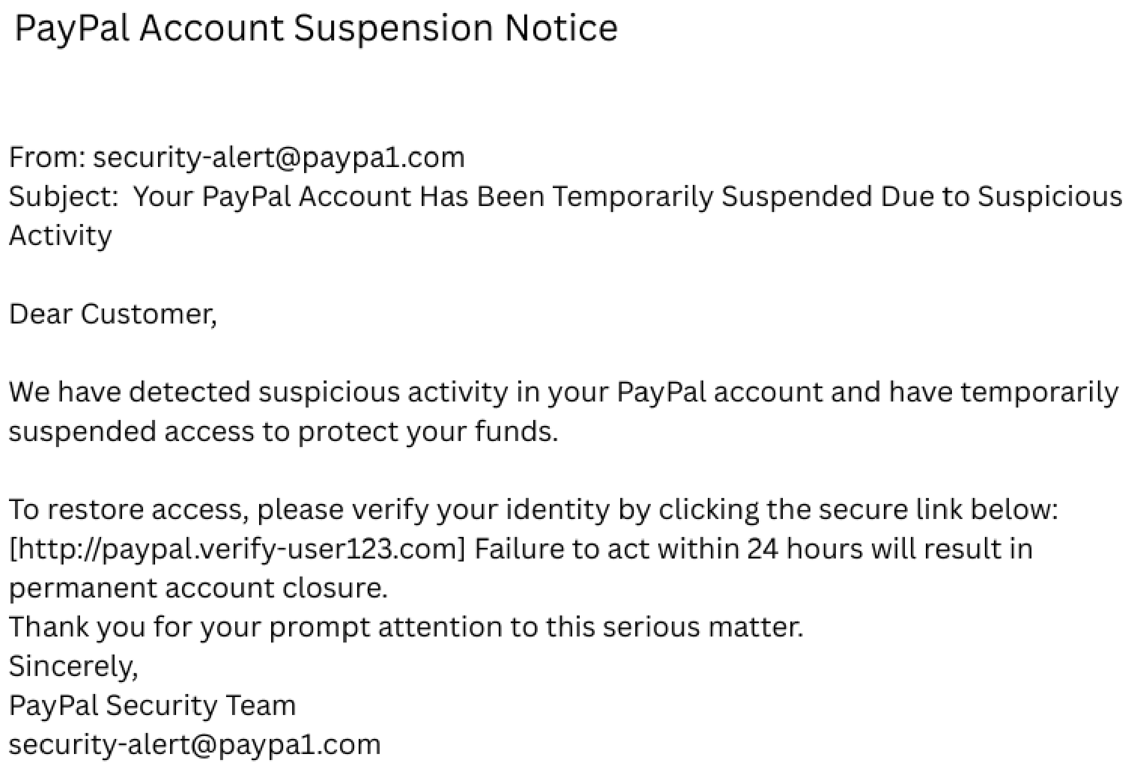
From: `security-alert@paypa1.com`

Subject: Urgent: Your PayPal Account Has Been Suspended

Link: `http://paypal.verify-user123.com`

Attachment: `Account_Verification_Form.pdf.exe`

Sample Email image:



PayPal Account Suspension Notice

From: security-alert@paypa1.com
Subject: Your PayPal Account Has Been Temporarily Suspended Due to Suspicious Activity

Dear Customer,

We have detected suspicious activity in your PayPal account and have temporarily suspended access to protect your funds.

To restore access, please verify your identity by clicking the secure link below: [http://paypal.verify-user123.com] Failure to act within 24 hours will result in permanent account closure.
Thank you for your prompt attention to this serious matter.
Sincerely,
PayPal Security Team
security-alert@paypa1.com

Phishing Indicators:

1. Sender Email Spoofing:

- Domain is `paypa1.com` (using the number “1” instead of “l”), not the legitimate `paypal.com`.

2. Suspicious Link:

- Visible link text says “Verify Account Now”

- Hover reveals: `http://paypal.verify-user123.com` — clearly a fake domain.

3. Urgent and Threatening Language:

- “Failure to act within 24 hours will result in permanent account closure.”

4. Unusual Attachment:

- Filename ends in `.exe` disguised as a `.pdf`, possibly containing malware.

5. Generic Greeting:

- Uses “Dear Customer” instead of the user's real name.

6.Social Engineering:

- Uses fear (account locked), urgency (24 hours), and authority (pretending to be PayPal) to manipulate the user.

Sample 2:

Microsoft Phishing Email Analysis

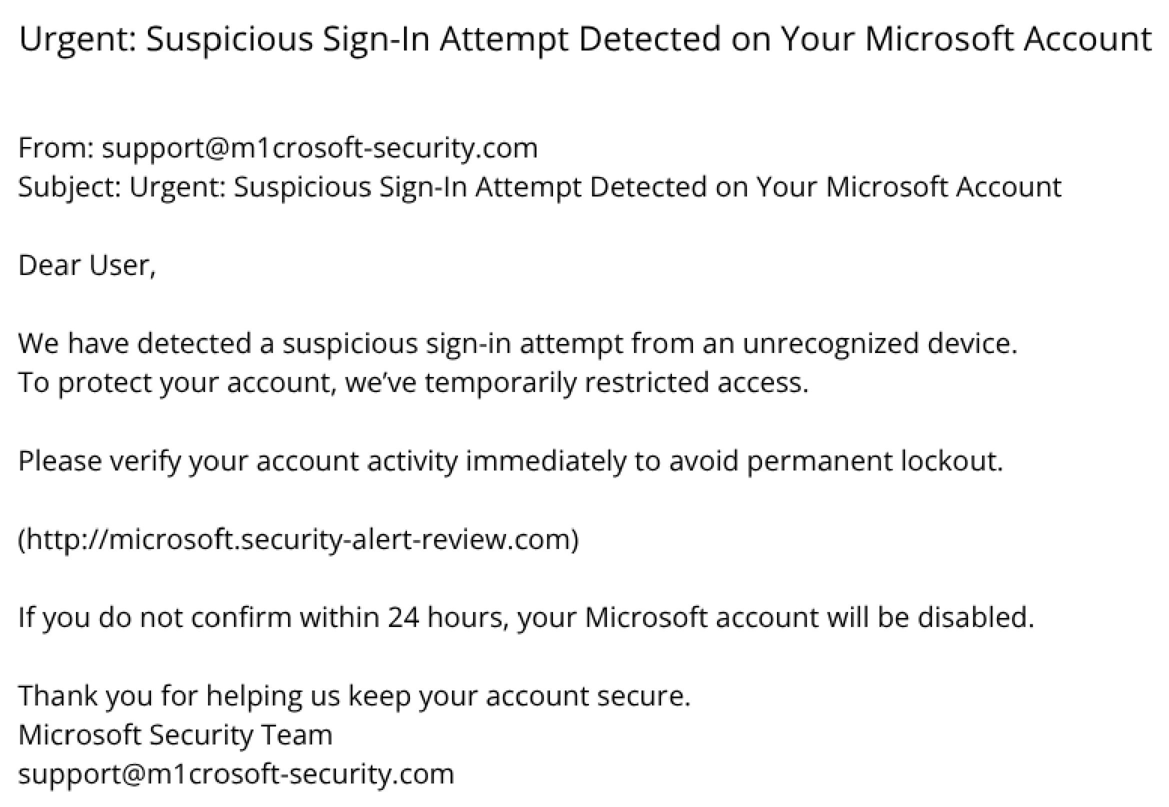
Fake Email Details

- From: support@m1crosoft-security.com

- Subject: Urgent: Suspicious Sign-In Attempt Detected

- Fake Link: http://microsoft.security-alert-review.com

Fake email image



Urgent: Suspicious Sign-In Attempt Detected on Your Microsoft Account

From: support@m1crosoft-security.com
Subject: Urgent: Suspicious Sign-In Attempt Detected on Your Microsoft Account

Dear User,

We have detected a suspicious sign-in attempt from an unrecognized device.
To protect your account, we've temporarily restricted access.

Please verify your account activity immediately to avoid permanent lockout.

(http://microsoft.security-alert-review.com)

If you do not confirm within 24 hours, your Microsoft account will be disabled.

Thank you for helping us keep your account secure.
Microsoft Security Team
support@m1crosoft-security.com

Phishing Indicators (Microsoft Email)

1. **Sender Email Spoofing:**
   - **Domain is m1crosoft-security.com — uses the number "1" instead of the letter "i" to mimic microsoft.com.**
   -
2. **Suspicious Link:**
   - **Visible link text says "Review Activity Now"**
   - **Hover reveals: http://microsoft.security-alert-review.com — not a legitimate Microsoft domain.**

3. **Urgent and Threatening Language:**
    - **“Please verify your account activity immediately to avoid permanent lockout.”**
4. **Generic Greeting:**
    - **Uses “Dear User” instead of the user's real name — a common phishing sign.**
5. **Lack of Contact Information:**
    - **No phone number or official support links provided — real companies always include support details.**
6. **Social Engineering Techniques:**
    - **Uses fear (account lock), urgency (24 hours), and trust manipulation (fake Microsoft branding) to pressure the user into acting quickly.**

Analysis with Tools

1. Email Header Analysis (MxToolbox)

- Return path mismatch found

- Untrusted mail server IP

- Screenshot: `header_analysis_mxtoolbox.png`

2. Link Reputation (VirusTotal)

- URL flagged as phishing by several engines

- Screenshot: `virustotal_link_scan.png`

3. Domain Check (URLVoid)

- Unknown registrar and suspicious host

- Screenshot: `urlvoid_result.png`

Conclusion:

This email exhibits typical phishing traits such as spoofed domains, urgency, and fake links. Using open-source tools helped confirm these risks.

Learning Outcome:

- Understood signs of phishing and how to identify email-based social engineering attacks.

- Improved skills in threat detection, header analysis, and domain inspection.

Tools Used:

- [MxToolbox Head Analyzer] (https://mxtoolbox.com/EmailHeaders.aspx)

- URL Hover Technique